

PRIVACY

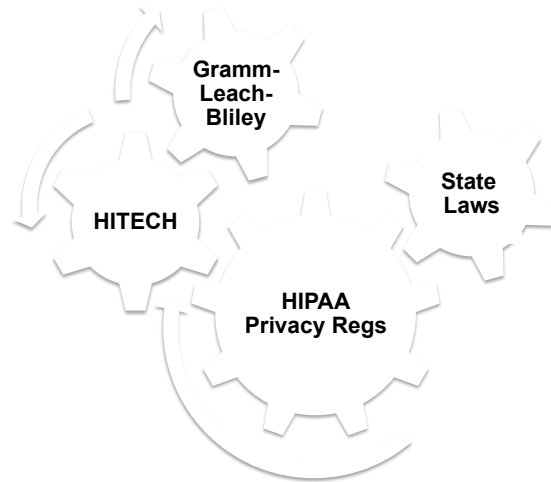
How HITECH expands obligations to protect consumer data

**Columbus Association of Health Underwriters
January 11, 2011**

Privacy – Protect and Defend

- **Privacy is the hot-button political issue of the new century**
 - Congress has already acted to protect the privacy of consumers' personal information
 - Gramm-Leach-Bliley Act (GLB)
 - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - HITECH provisions of American Recovery and Reinvestment Act (ARRA)
 - Regulators have already moved forward with other protections
 - Junk mail, spam, no-call lists, Red Flag Rules

Privacy Protections Impacting Agents



3

Gramm-Leach-Bliley

- **Applies to “financial institutions” and those who sell products for financial institutions**
 - Banks and insurance companies
 - Insurance agents
- **Financial institution safeguards**
 - Disclosure obligations
 - Privacy policy obligation
 - Privacy notice requirements

GLB Privacy Protections

Banks, Insurance Companies and Agents

- May not disclose non-public personal information (NPPI) to non-affiliated third parties without:
 - Notice to clients
 - Opportunity for clients to opt out
- What is “non-public personal information”
 - Personally identifiable information...
 - collected from consumers
 - collected about consumers
 - resulting from a transaction with consumers

Gramm-Leach-Bliley Exceptions

- **Exceptions to GLB privacy protections**
 - Joint marketing
 - Redisclosure and Reuse of Information

Safeguarding Customer Information-GLB

- **Protect what you have about your clients**
 - Assess and know what information you have
 - Manage and control risk to your business
 - Access rights to customer information
 - Encryption of information
 - Contract provisions for service providers

Rulemaking and Enforcement-GLB

- **Numerous federal agencies have regulatory and enforcement responsibility**
 - Federal Reserve Board
 - Comptroller of the Currency
 - Federal Deposit Insurance Corporation
 - Office of Thrift Supervision
 - National Credit Union Administration
 - Securities and Exchange Commission
 - Federal Trade Commission

Applicability of State Law-GLB

- **You are also subject to the jurisdiction of the state insurance regulatory authority**
- **States may enact stronger measures**
- **Many states require additional protections:**
 - Opt in
 - Consumer access to information and correction rights
 - Affiliate sharing on sharing of
 - Limitations on disclosure of medical information

HIPAA' s Privacy Rule

Introduction to HIPAA

- **Why do we need it?**
 - Electronic transactions simplify the claims, enrollment, eligibility, and inquiry processes
 - Reduce (manage) the high cost of administering healthcare claims
 - Increase trust with privacy and security measures
 - Good business and confidentiality practices

Who Does HIPAA Apply To?

COVERED ENTITIES

- **Health Plans**
 - Self-insured health plans - the plan sponsor
 - Fully insured health plans - the insurer as well the plan sponsor
- **Providers**
 - Doctors, hospitals who transmit oral or written health information
- **Data Clearinghouses**
 - Exchanging data between providers and health plans

Who Does HIPAA Not Apply To?

- **Business Associates**
 - Third parties who receive information from a covered entity
 - Must have an agreement (more later)
 - Includes insurance agents working on health insurance products and health plans
- **This is one area changing due to HITECH because business associates, by signing an agreement, are directly responsible for any privacy violations**

Key HIPAA Terms

Covered Entity

- Healthcare provider, clearinghouse, health plans that conducts covered transactions (Not who you are, but what you do)

Business Associate

- Person, group or organization that handles PHI on behalf of a Covered Entity

Notice of Privacy Practices (NPP)

- Notice describing how you will protect employee health information

Protected Health Information (PHI)

- Health information + information that identifies the employee

HIPAA Does Not Regulate

- Short-term and long-term disability
- AD&D (Accidental Death and Dismemberment)
- Life insurance
- Worker's Compensation
- Americans with Disabilities Act (ADA)
- Fitness-for-duty exams (DOT or OSHA exams)
- Drug testing
- Work-life benefits (on-site clinics; fitness center)
- Family Medical Leave Act (FMLA)
- Auto medical insurance

HIPAA Privacy Regulations

- **General Rule:**
 - “Covered entities” may not use or disclose an individual's “protected health information” without the authorization of the individual unless specifically required or allowed by the privacy regulation.

Overview of the Privacy Rule

- **Protects PHI in ANY form (oral, written, electronic)**

- **Requires policies and procedures to manage collection, storage, handling, and transmission of PHI**

- **Requires you develop contracts and agreements with Business Associates that handle PHI**

- **Gives employees rights over their PHI**

Protected Health Information (PHI) In the Workplace

PHI	Not PHI
Employee health information on benefit enrollment form	Benefit enrollment form with no health questions or information
Employee requests help on health claim	Pre-employment or random drug test
Employee gives reason for sick leave	Information for Worker's Comp claim*
Old health enrollment forms	FMLA Notices

*If denied, any additional health information becomes Protected Health Information

Business Associates

- **Person, group or organization that handles PHI on your behalf**
- **Is not an employee and does not fall under direct supervision of Covered Entity**
- **Must ensure that they will protect PHI**
- **Must ensure that any of their subcontractors will protect PHI**

Business Associate Agreements

Business Associate	Reason for agreement
Insurance Agent	To allow your insurance agent to have access to PHI of your employees
Third Party Administrator (TPA)	To allow the TPA to facilitate the administration of your employee benefit plan
Lawyer or CPA, who sees PHI	For the purposes of reviewing claims or information necessary for a business purpose

Enforcement Agency for Privacy Rule

```

graph TD
    OCRC((HHS Office for Civil Rights)) --- CF((Complaint Form))
    OCRC --- G((Guidance))
    OCRC --- FAQ((Frequently Asked Questions))
    OCRC --- PR((Privacy Rule))
    OCRC --- FS((Fact Sheets))
    OCRC --- EM((Educational Materials))
    
```

Office for Civil Rights website:
www.hhs.gov/ocr/hipaa

Penalties for Privacy Rule Violations

Violation	Penalties
General	\$100 / day/ incident, up to \$25,000/ year
Criminal penalties	\$50,000 + one year prison
False pretenses	Up to \$100,000 + 5 years
Intent to sell, \$ gain, harm	Up to \$250,000 + 10 years

Updated Regulations: Marketing

- **Agents may not use an individual's PHI for marketing purposes without prior written authorization, except:**
 - Face-to-face meetings
 - Promotional gifts of nominal value
- **“Marketing” - any communication by an agent that encourages an individual to use a product or service.**

Permissible Communications

- **Health-related communications to plan enrollees that HHS does not consider to be marketing**
 - Communications about network participating providers and health plans
 - Services offered by a provider
 - Benefits covered by a health plan
 - Products or services provided by a covered entity
 - Communications regarding an individual's treatment, case management or care coordination
 - Directions or recommendations for alternative treatments, therapies, or healthcare providers (such as specialist referrals)

Incidental Use & Disclosure

Incidental uses or disclosures are not violations of the Rule provided that the covered entity has met the reasonable safeguards and minimum necessary requirements.

- Client talks to an agent in a lobby and the discussion is overheard
- Do not have to disclose in privacy notices to patients/clients that incidental disclosures may occur

New Actions on Employee Privacy

- **Culture changes**
- **What you can and cannot say**
- **May take about six months to change behavior**
- **Sanctions**
- **Retrain – new employees, job change**

How it Affects Agents - Summary

- **Business Associates Agreements needed with carriers and clients**
- **Summary health information may be shared by plan with agent for enrollment without HIPAA infrastructure**
- **If more detailed data is required, PHI may be used for health underwriting without an authorization**
- **PHI cannot be used for non-health coverage purposes (life, long term disability, etc) without an authorization**
- **Agents cannot share PHI with national claims databases (e.g. Medical Bureau)**

HIPAA' s Security Rule

Purpose of the Security Rule

- **Protect electronic patient health information (PHI) in three ways:**
 - Confidentiality - PHI concealed from people who do not have the right to see the information
 - Integrity - information has not been improperly changed or deleted
 - Availability - healthcare provider can access the information when it is needed
- **As originally adopted, HIPAA Security Rule only applied to Covered Entities (not BAs)**

Why a Security Rule?

- **Protecting PHI becomes more important as healthcare providers transition to Electronic Health Records**
- **Increasingly important with increased use of technology for data transmission**
 - Emails
 - Electronic enrollments

Three Security Rule Standards

- **Administrative Safeguards**
- **Physical Safeguards**
- **Technical Safeguards**

Specific Staff Expectations

- **Manage passwords**
 - Have staff members choose and remember
 - Change passwords regularly
 - Notify ISO if concerned that password is being improperly used by someone else
- **Identify and keep out malicious software**
- **Use workstations properly**
- **Know sanction policies**
- **Learn and follow policies and procedures**

Use Workstations Properly

- **Position monitors so others, especially visitors, cannot see the screen**
- **Log off workstation (or activate the password- protected screen saver) when**
 - Finished with tasks
 - Leaving the area and can't see the workstation

Use Workstations Properly (cont' d)

- **When an idle workstation is already logged onto the network by someone else and you are going to use it:**
 - Log off
 - Log on with your own password
 - Remind whoever did not logoff that doing so is against the policy

Use Workstations Properly (cont' d)

- **Threats to the network**
 - Devices introducing viruses into the system - CDs, floppies, iPods, USB drives, PDAs
 - Family members or friends using the computers in off-sties can introduce viruses and expose patient data.
 - Web surfing for personal enjoyment
 - Downloading free programs or music from the Internet on office machines can introduce viruses.

Use Workstations Properly (cont' d)

- **Protect the business**
 - Follow the policies about what you put in emails and when you delete them
 - Encrypt documents for storage and transmission as directed
 - Put a password protected time-out on all portable devices since they are frequently lost or stolen
 - Report the loss of any equipment which might contain identifiable health information

Learn and Follow the Policies and Procedures

- **Adopt policies and procedures**
 - Who has access to what portion of the network and data.
 - What should be encrypted when
- **Easily accessible by every employee**
- **The policies outline that every employee, especially management, is responsible for knowing and carrying out the relevant policies that affect the business.**

Know the Sanction Policies

- **The business must have and enforce a written sanction policy**
- **Unintentional and intentional infractions must be documented and action taken in response.**

Consequences for Violations

- **Intentional infractions may lead directly to dismissal**
- **Infractions can result in civil and governmental penalties for the violator**
 - as well as for those responsible for implementing and monitoring the security policies
- **Knowingly misusing patient information (in electronic form or any form) is a felony under HIPAA**

HITECH Provisions of ARRA

HITECH

- **Congress passed HITECH provisions as Title XIII of ARRA in February 2009**
 - Most significant change to the healthcare privacy and security environment since the original HIPAA privacy rule
 - Congress finally acted – “HIPAA with teeth”
 - Did not change everything – but changed a lot

43

HITECH

- **Congress passed provisions as Title XIII of ARRA**
 - Most provisions will require further regulatory clarification
 - Meaning that the regulatory bodies are not yet finished with their process
 - Likely the regulatory process will fall on the side of greater privacy protections

44

HITECH – Eight Major Changes

• **Notice of security breaches**

- Breach: the unauthorized acquisition, access, use or disclosure of protected health information (PHI).
- Must provide notice not less than 60 days from discovery of the breach
- This information is covered more fully in the Breach Notification Presentation in this package.

1

45

Security Breach Notifications

- **Breach: An individual's protected health information [in "unsecured" form] that has been, or is reasonably believed by the covered entity to have been accessed, used, acquired or disclosed to an unauthorized person, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.**
 - Exceptions:
 - Unintentional access by employees or individuals acting under authority of covered entity or business associate if information is not used or disclosed by recipient or anyone else.
 - Inadvertent disclosure from one covered entity or business associate employee authorized to access PHI to a co-employee authorized to access PHI
 - Unauthorized access by an unauthorized person who cannot reasonably be able to retain the information disclosed.

46

Security Breach Notifications (con't)

- **These rules apply to Protected Health Information (PHI) in any format**
 - ePHI (electronic PHI)
 - Paper
 - Tapes/CDs

- **Rules do not apply to PHI in an “secured” form**
 - If improperly acquired data was secured (encrypted or destroyed), then no breach notification is required

47

When There is a Breach

- **Notification when there has been a breach above the “harm threshold”**
 - Responsible for determining whether a breach poses a “significant” risk and warrants notification.
 - Do a risk assessment:
 - What and how much information was released?
 - Can we get it back?

- **Notify without unreasonable delay and at least within 60 day timeframe**
 - 60 days begins to run from the date the covered entity or business associate or any employee, officer or other agent of the covered entity or business associate knew or reasonably should have known about the breach ⁴⁸

What Needs to Happen

- **Method of notice (new obligations):**
 - Send a written notice to the individual (or next of kin, if the individual is deceased) at the last known address by first-class or electronic mail.
 - Post a conspicuous message (for a period determined by HHS) on your Web site's home page or with major print or broadcast media when insufficient or out-of-date contact information prevents direct contact.
 - Call individuals whose unsecured health information was breached when there is an imminent threat of misuse.
 - Notify prominent media outlets within the state or jurisdiction if a breach of unsecured PHI affects or is reasonably believed to affect more than 500 residents.
 - Notify HHS immediately for breaches involving more than 500 individuals and annually for all other breaches.

49

Designing the Content

- **Content of notice**
 - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - A description of the types of PHI involved in the breach (such as full name, social security number, date of birth, home address, account number, diagnosis, disability code, etc.);
 - Suggested steps individuals should take to protect themselves from potential harm resulting from the breach;
 - A brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 - Contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, and postal address.

50

HITECH – Eight Major Changes

- **HIPAA Applies to Business Associates** **2**
 - This means you!
 - Before – covered entities only; Now: you are under the regulatory authority of HHS for all of the requirements of the HIPAA Privacy and Security Rules
 - Business Associates may include employers, third party administrators, wellness and disease management, utilization and subrogation vendors, among others.

51

HITECH – Eight Major Changes

- **HIPAA Applies to Business Associates** **2**
 - Act contains contract mandates that require Business Associate agreements to be rewritten
 - Business Associates subject to same civil and criminal penalties applicable to Covered Entities
 - When effective:
 - Fines: immediately
 - Contract changes: 1/2010

52

HITECH – Eight Major Changes

• “Minimum Necessary” Changes **3**

- The current rule requires covered entities to only use and disclose the minimum amount of PHI necessary to accomplish a permitted purpose.
- HITECH Act seeks to clarify the minimum necessary provision to limit disclosure to
 - the extent practical, uses and disclosures must be limited to the “limited data set”; or
 - if needed by such entity, to the minimum necessary to accomplish the intended purpose.

53

HITECH – Eight Major Changes

• “Minimum Necessary” Changes **3**

- Secretary of HHS is required to issue further guidance on “minimum necessary” disclosures from covered entities to business associates.
- Guidance shall take into consideration information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

54

HITECH – Eight Major Changes

• Stiffer Penalties for Noncompliance **4**

- Situation #1: CE/BA did not know or would not have known through exercise of reasonable discretion
 - Minimum: \$1,000 per violation – Max of \$25K for all violations
 - Maximum: \$50K per violation – Max of \$1.5M for all violations
- Penalties may be waived or mitigated if violation is corrected within 30 days of date discovered

55

HITECH – Eight Major Changes

• Stiffer Penalties for Noncompliance **4**

- Situation #2: Violation due to willful neglect but timely corrected
 - Minimum: \$10,000 per violation – Max of \$50K
 - Maximums: \$250K per violation – Max of \$1.5M
- Situation #3: Violation due to willful neglect
 - \$50K per violation with no maximum
 - What is “willful neglect”?
 - Must be defined within 18 months; enforced within 24 months

56

HITECH – Eight Major Changes

• **Mandatory Enforcement**

- HHS is required by law to formally investigate complaints if preliminary investigation of complaint suggests Willful Neglect
- Provides explicit authority for state attorneys general to enforce HIPAA Privacy and Security regulations
- Compliance audits are required to be conducted periodically
 - Adopted because of the low “complaint-to-investigation” ratio during past 5 years

5

57

HITECH – Eight Major Changes

• **Attorney Fees Coming?**

- HHS is permitted to adopt regulations which would permit penalties collected to be “shared” with victims
- Apparent authority to have those fines to be given, in part, to victim’s attorney
- HHS must “answer” the question about fine sharing by 2012
- Guess who’s excited about this?

6

58

HITECH – Eight Major Changes

- **Notice of Agency's Privacy Protection** **7**
 - Advised that Business Associates provide notice of privacy practices to its clients
 - Goes along with existing obligation to provide notice under GLB
 - No explicit requirement at this time that clients sign acknowledgement of receipt
 - ...however may be a good practice
 - The package includes the model notice of privacy practices for our agency to use

59

HITECH – Eight Major Changes

- **Criminal Enforcement** **8**
 - HIPAA Privacy: only applied to covered entities
 - HITECH: Criminal provisions apply to any individual, regardless of whether they are a covered entity
 - Employees of Covered Entity
 - Business Associates
 - Employees and Third Parties of Business Associates

60

HITECH Compliance “To Do List”

- **Remember: these rules apply to you!**
- **Privacy compliance deadline: 2/17/2010**
 - Amend business associate agreements with group health plans to include additional required provisions
 - Cure your breaches of Business Associate agreements
 - Enter into Business Associate agreements with privacy safeguards by 2/17/2010 with any organization that provides data transmission services to you

HITECH Compliance “To Do List”

- **Privacy Compliance: 2/17/2010 (cont’ d)**
 - Comply with new HITECH minimum necessary requirements effective 2/17/2010 (further HHS guidance expected by 8/17/2009)
 - Comply with changes to request for restriction rules
 - Comply with new marketing restrictions
 - Seek authorization prior to selling PHI for certain purposes (beginning no later than 2/17/2010, depending on when regulations are issued)

HITECH Compliance “To Do List”

- **Privacy Compliance: 2/17/2010 (cont’ d)**
 - Start accounting for disclosures of Protected Health Information for non-treatment, payment or health care operations purposes immediately
 - Permit access to PHI in electronic format if you hold electronic health records, presumably effective 2/17/2010

HITECH Compliance “To Do List”

- **Security Compliance – 2/17/2010:**
 - Implement all HIPAA security administrative, technical and physical safeguards
 - Wait for HHS guidance (expected by 1/1/2010 and to be updated annually) regarding the most effective and appropriate technical safeguards and consider implementing
 - Wait for HHS guidance on the technologies or methodologies that make PHI secure and consider implementing

HITECH Compliance “To Do List”

- **Security Compliance:**
 - Comply with new notification rules for breach of unsecured PHI
 - Likely to be 30 days after regulations are issued relating to the technologies or methodologies that make PHI secure (regulations due by 8/16/09 so notification requirements will apply no later than 9/15/09)
 - Appoint a security official
 - Conduct a security risk analysis
 - Purchase Security Kit from Simplified Training
 - www.simplifiedtraining.com

HITECH Compliance “To Do List”

- **Security Compliance:**
 - Develop and maintain written security policies & procedures
 - Amend business associate agreements to include new security rules (as early as 9/15/2009 since that is the latest date the new breach notification rules will apply)
 - Enter into business associate agreement with security safeguards with any organization that provides data transmission services to you
 - Conduct privacy and security workforce training

Questions?